الهاتف المحمول ... الخطر القاتل



لقد كانت الهواتف المحمول نعمة في تيسير التواصل وتقريب المسافات، غير أنها تنقلب لنقمة عندما يمس الأمر أمنك وحياتك وخصوصيتك، وتسريب المعلومات الخاصة بالفرد والجماعة وعملها على حد سواء، وفي هذه الدراسة المختصرة نقف على بعض مخاطر الجوال مستعينين ببعض النماذج التي كان الجوال سببا في الإيقاع بها، وقبل ذلك نُذكر بقاعدتين أمنيتين وهما (الاجتهاد في الأمن ممنوع) و(نفذ ما تسمع وليس ما تفهم).

أولاً : أن أجهزة الاتصال (الجوال) تعتمد على الخلايا (الأبراج وأنتينات وخلايا الإرسال) الموزعة في أنحاء مختلفة قريبة من استخدامات الناس، وبالتالي فإن هذه الخلايا تقوم بعملية (Hand Over) وتعني تسليم المشترك من أقرب برج إلى البرج الذي يليه تلقائياً، ومع كل انتقال يتم تجديد بياناتك وإعطاء أخر البيانات عنك.

ثانياً : ماذا يستقبل برج ومقسم الاتصالات من جوالك:

مع بدء تشغيل الجوال يقوم جهازك باستشعار أقرب موقع للخدمة ومن ثم يعطيه المعلومات التالية:

١. معلومات وبيانات كاملة عن المشترك وفقاً لمعلومات تسجيل الشريحة لدى الشركة، إضافة إلى بيانات عن نوعية الجهاز المستخدم، ورقمه والموديل، وتاريخ التصنيع.... الخ. (وهذا يعني أنك لو استخدمت شريحة جديدة في جهاز مستعمل من قبل على شريحة سابقة مُراقبة فإن هذه الشريحة الجديدة ستُعرف بسبب معرفتهم لمواصفات الجهاز الذي استخدمت به الشريحة الأولى المراقبة).

٢. يعطي معلومات عن أقرب مقدم خدمة لك (برج الإرسال).

٣. يمكن لأبراج الاتصال أن تحدد النقطة التي أنت فيها وارتفاعها عن سطح الأرض، أما الأجهزة التى فيها خاصية GBS فإنه يتعامل مع خطوط الطول والعرض وهو يحدد إحداثية المتصل بدقة تصل إلى حجم الجهاز.

٤. في حالة إقفال الجهاز وفصل الطاقة عنه يعطي آخر نقطة كان متواجد بها ويتوقف عن بث الإشارات التي تحدد مكانك وليس منع نقل الأصوات، فإذا أغلقت الجهاز دون فصل البطارية فمن الممكن التجسس عليك.

نموذج حقيقي

- نقدم لكم نموذج حقيقي ومُدعم بالصور من ملف مراقبة الأخ «أبو عمر المصري» التي آلت إلى اختطافه من قبل الـ CIA حيث تم اختطافه من ايطاليا ثم رُحل إلي ألمانيا ثم من خلال طائرة صغيرة إلي مصر، وكل ذلك دون علم السلطات الرسمية الايطالية التي لم تعلم بمكان أبو عمر المصري إلا بعد ١٤ شهر من خلال أن زوجته جاءها اتصال من مصر يفيد أنه تم الإفراج عن أبو عمر من قبل السلطات المصرية بعد ١٤ شهر من التعذيب والتحقيق.

- وبعد ذلك بدأت السلطات الإيطالية بعمل تحقيق كامل في هذا الحادث, ومن خلال التحري والبحث وصلت إلي أخر مكان تواجد فيه «أبو عمر».

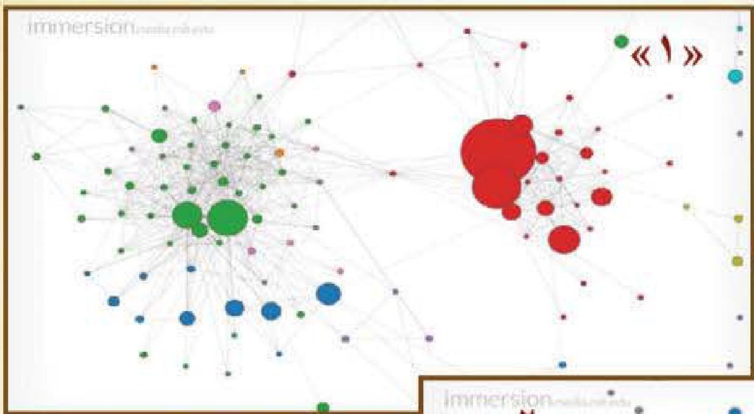
- فكانت بداية لعملية بحث وتحري جديدة حيث قامت السلطات الايطالية بعملية جرد كامل لكل المكالمات والرسائل الهاتفية الصادرة والواردة وكذلك المراسلات البريدية عبر الانترنت، وهذا يكون من خلال برامج خاصة تعتمد على كميات كبيرة من أنماط البيانات والارتباطات، حيث تم اكتشاف أنه في هذا المنطقة كان هناك ٣٥ هاتف و١٨ شخص يتواصلون مع بعضهم البعض وأنه تم استخدام هذه الهواتف من خلال هؤلاء الأشخاص لمدة شهرين قبل عملية الاختطاف ويومين بعدها حيث تم إغلاقها بعد ذلك.

- وتبين أنه هذه الهواتف كانت تستخدم بين هؤلاء الأشخاص فقط، وانه في ليلة الاختطاف ظل أحد هذه الهواتف مغلق وداخله البطارية لمدة ٨ ساعات في أحد

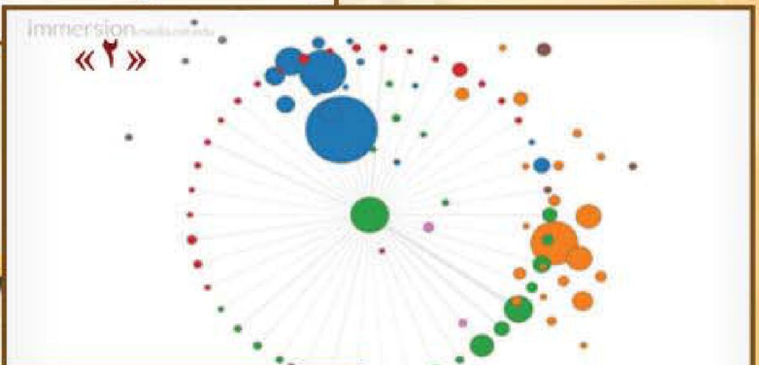
يُتبع ‹‹‹

الفنادق مما ساعد في تحديد مكانه وهو أحد الفنادق المعروفة في المنطقة وبعد التوجه إلي هذا الفندق عُرف أنه كانت هناك غرفة محجوزة باسم ضابط أمريكي قام بالحجز باسمه الحقيقي في هذا الفندق ومن خلال التحري والتحليل أيضا عرف أن هؤلاء ١٨ شخص يحملون فيز تحمل أرقام متشابهة ومتسلسلة. كذلك تم رصد أحد المكالمات بين أحد هؤلاء الأشخاص وبين ضباط ألCIA في المقر الرئيس في أمريكيا، فتم الكشف عن هذه المجموعة كلها وكان عددها ١٨ شخص دخلوا ايطاليا و ٤ أشخاص مسئولين عن العملية داخل واشنطن نفسها. وتم الحكم عليهم في ايطاليا غيابيا بالسجن ٥ سنوات ومتهم واحد ٨ سنوات وثلاثة منهم تم تبرئتهم لوجود حصانة دبلوماسية معهم.

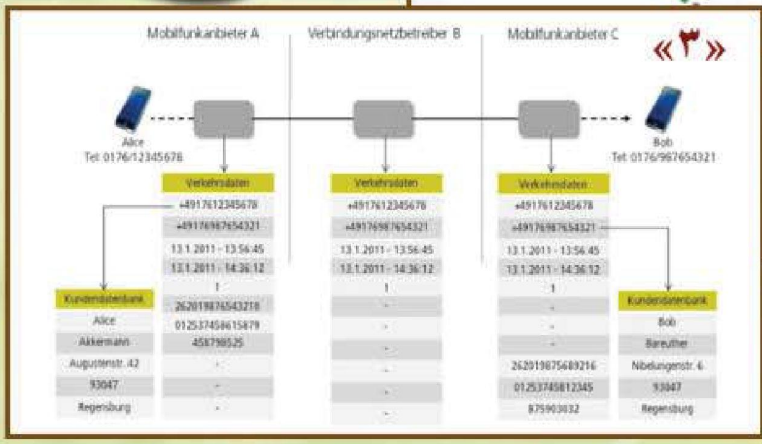
ومن هنا يظهر مدى خطورة استخدام أجهزة الاتصال وسهولة تحديد أماكن وهوية أصحابها وبدقة وتفاصيل كبيرة، واليكم بعض الصور التحليلية التي يستطيع هذا البرنامج رصدها وتحليليها.



الصورة الأولي:
وهي تشمل رصد كل المكالمات التي أجريت، واتجاهها والربط بين الاتصالات وحلقات الاتصال المشترك.



الصورة الثانية:
رصد الاتصالات بين أشخاص عديدة جميعهم يتصلون بشخص واحد، حيث يتم من خلال ذلك تحديد الحلقة المركزية أو القائد والمسئول.

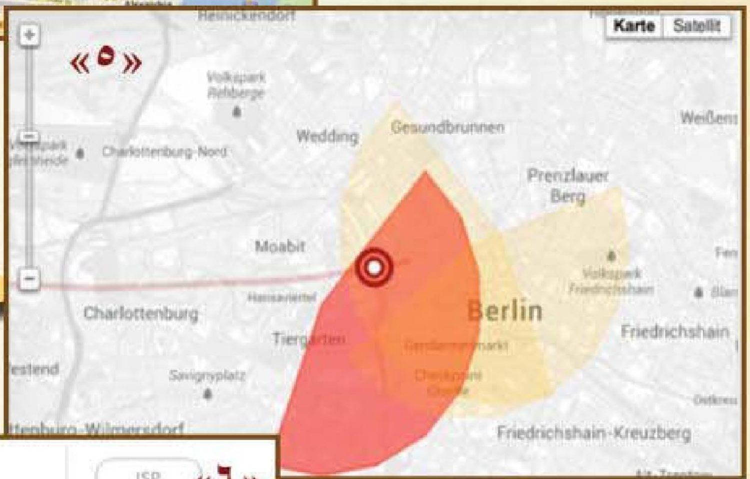


الصورة الثالثة:
تشمل معلومات تفصيلية عن مكان وزمان وأرقام ورسائل الاتصال بين شخصين.

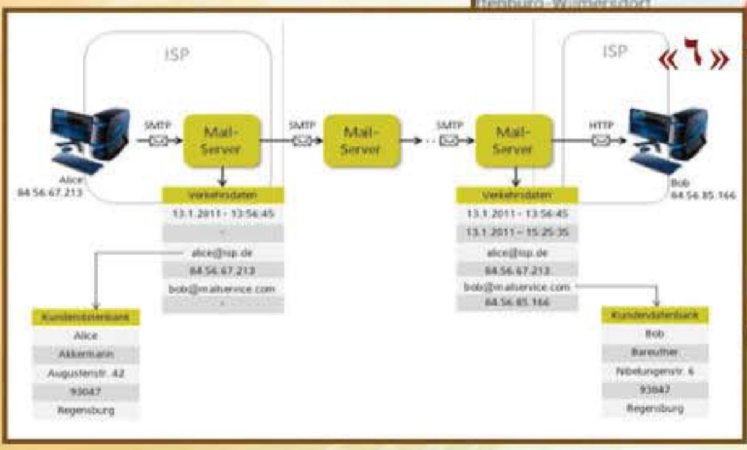
يُتبع ›››



الصورة الرابعة:
تحديد أماكن الأشخاص وتحركاتهم وزمن ومدة تحركاتهم من خلال الأقمار الصناعية.



الصورة الخامسة:
تحديد مكان الشخص المعني فيه بوضوح كبير ودقة عالية و تحديد المكان بالمدينة والشارع والبيت وأدق من ذلك.



الصورة السادسة:
تجسس وتتبع المراسلات البريدية عبر الانترنت حيث يتم تحديد مكان وزمان فتح الإميل وكذلك تحديد تاريخ إنشاء الإميل وعدد الرسائل المرسلة والواردة إليه.

تحذيـر:

أخي المجاهد، أنت مراقب مراقبة لصيقة وعلى مدار الساعة، فأنت مطلوب، وعدوك يمتلك أدوات المراقبة والقتل، لذا لا بد من إجراءات صارمة لا فرصة فيها للمصادفة.

التوصيـات:

١- يمنع استخدام أجهزة الاتصال في أي مهمة كانت، ويفضل تركه في المنزل وعدم إغلاقه عند الخروج.
٢- في أي مهمة خاصة عدم ترك أي أثر (اسم – وثيقة – رقم – عنوان) تدل على هويتك وشخصيتك الحقيقية نهائيا.
٣- لا تجعل رقمك مفتوح للجميع، وإذا شعرت أن أحدهم حصل على رقمك فحاول أن تتخلص من الشريحة والجهاز بسرعة.

هذا والله أعلى وأعلم... سائلين الله تعالى القبول والإخلاص في القول والعمل

جمع وترتيب أخوكم : أبو عامر

كيف تحمي جهازك الشخصي (١)

بقلم: قسورة حفظه الله

مع تطور التكنلوجيا الرقمية ويعد أن أصبحت جزءًا لا يتجزأ من الحياة اليومية للفرد، أصبح جزء كبير من تركيز أجهزة المخابرات العالمية على كيفية جمع المعلومات عنك عبر نقطة الضعف هذه (أي ارتباطك بالتكنلوجيا على مدار الساعة)، وقد خصصت هذه الأجهزة المخابراتية معامل ضخمة لهذا الأمر وفرغت في سبيل ذلك عشارات آلاف من الخبراء التقنيين وأصبح جزء كبير من ميزانيات تلك الأجهزة تُنفق عليه، فهو يعتبر مصدر لكنز من المعلومات لم تحلم به هذه الأجهزة من قبل، فما بالك بمجموعة من الجواسيس يرافقونك ليل نهار خطوة بخطوة، يسمعون كل كلمة تخرج منك وكل كلمة تكتبها وكل رسالة تقرأها ويعلمون تفاصيل شبكتك الاجتماعية والتنظيمية ... الخ

أولا: التجسس عليك عن طريق نظام التشغيل (الويندوز):

اعلم أخي المجاهد أن أجهزة المخابرات ليست ساذجة كي تأتيك ببرمجيات الاختراق بشكل علني أو حتى مريب، بل يتم استخدام طرق لحقن نظام التشغيل بطرق خبيثة ومخفية ببراعة بحيث لا يتم اكتشافها، إليك بعض هذه الطرق وكيفية الوقاية منها:

طريقة الاختراق	التعريف والوظيفة	أقوى البرامج المضادة
برمجيات خبيثة	تسمى Malware أو spyware وعمل هذه البرمجيات هذ التخفي بين برامج نظام التشغيل بغرض جمع المعلومات، وقد تستخدمها أيضا شركات دعائية لتجمع عن المستخدم معلومات لتستهدفه فيما بعد بإعلانات توافق اتجاهاته، ولهذه البرمجيات الخبيثة برامج خاصة للتخلص منها وتسمى anti-spyware أو anti-malware عمل هذه البرمجيات هي جمع المعلومات عن المستخدم، وقد تستخدمها أيضا شركات دعائية لتجمع عن المستخدم معلومات لتستهدفه فيما بعد بإعلانات توافق اتجاهاته	Malwarebytes أو Ad-Aware Free +Antivirus
برامج تسجيل ضربات لوحة المفاتيح	تسمى برامج key-logger وهذه البرامج لا يتعرف عليها مضاد الفيروسات أو مضاد البرمجيات الخبيثة كتهديد لأنها برامج مرخصة! ووظيفتها تسجيل الأحرف التي يتم ضربها على لوحة مفاتيحك مع تسجيل التوقيت ووضع الجهاز الحالي مثل على أي موقع تتواجد، ما هي البرامج المفتوحة، ويوجد برامج تحمي المستخدم من هذا التطفل وتسمى ant-logger	Zemana AntiLogger
الفيروسات	وهي ملفات أو برمجيات تصيب الجهاز وهدفها الأول هو التخريب، وقد يستخدم لضرب منظومة الحماية وإضعاف الجهاز حتى يسهل عمل البرمجيات الخبيثة spyware التي تكلمنا عنا سابقا، ويمكن أن تقوم هذه الفيروسات أيضا بمهمات جمع المعلومات والمراقبة والبرامج المضادة تسمى برامج antivirus	Bitdefender أو Kaspersky

بالإضافة لما سبق من الضروري جدا أن يكون مثبت على جهازك برنامج يسمى الجدار الناري أو firewall ووظيفة هذا الجدار الناري هو منع أي تصرف مشبوه أو غير اعتيادي على الدخول إلى برامج النظام، أي انه يعمل رقابة عامة وفلترة على الاتصالات الصادرة والواردة من جهازك بحيث لا يسمح بأي نشاط إلا بموافقتك أنت، ومن اقوى هذه البرامج التي ننصح بها: Comodo Firewall أو ZoneAlarm Free Firewall.

هذا كله لا يغني عن أن يكون لديك أخي المجاهد «حس أمني» بالتعامل مع ملفاتك ومعلوماتك الحساسة على جهازك، وحفظها بطرق مشفرة، وسنفرد لهذه الطرق درس كامل بإذن الله.

لمزيد من المعلومات يمكنكم التواصل مع الأخ: قسورة

@qswra4wmqx

كيف تحمي جهازك الشخصي (٢)

بقلم: قسورة حفظه الله

الحمد لله والصلاة والسلام على رسول الله، أما بعد...

تطرقنا في الدرس السابق الى أساليب الإختراق والتجسس على المستخدم عن طريق إختراق نظام التشغيل (ويندوز) وكيفية الوقاية وحماية النظام، وهي خطوات هامة لا يجب تجاوزها لمن أراد أن يحمي جهازه الشخصي من التجسس والاختراق، ولمن فاته يمكن الرجوع الى العدد السابق من مجلة الوعد الأخر.

~~أولا: التجسس عليك عن طريق نظام التشغيل (الويندوز)~~

ثانياً: تأمين تصفح الإنترنت (تأمين المتصفح)

إن المتصفح هو نافذتك الخارجية الى العالم الافتراضي والشبكة العنكبوتية، و90% من الاختراقات قد تأتيك من هذه النافذة، فوجب تامين المتصفح جيدا لعزله عن الوصول الى داخل النظام قدر الإمكان، لا بد قبل البدء بالتطبيق العملي ان يم ذكر باختصار ما هي اساليب الاختراق عن طريق المتصفح:

١. الاختراق عن طريق استغلال الثغرات في المواقع.

٢. عن طريق تتبع نشاط المستخدم على النت، وهذا سهل جدا ولا يحتاج جهد.

٣. عن طريق زرع (كوكيز) مهمتها جمع معلومات حول المستخدم.

٤. مواقع مثل جوجل تجمع عن المستخدم عادات البحث اليومية للمستخدم ومعرفة اهتماماته.

٥. بعض المواقع تكون مصابة وتعمل على اختراق المستخدم عن طريق تنزيل برمجيات خبيثة.

٦. جمع معلومات حول المستخدم مثل الموقع الجغرافي والأي بي ونوع المتصفح وبعض خصائص الجهاز والشاشة والبرامج المثبتة على الجهاز.

٧. مواقع مزورة.

٨. الإعلانات.

هل تعلم؟! حسب اتفاق جوجل وفيسبوك مع الحكومة الامريكية انه يحق للحكومة الأمريكية طلب كافة بيانات ومعلومات المستخدم بما في ذلك نشاطاته وعاداته وعلاقاته وكلمات سره من هاتين الشركتين، في عام ٢٠٠٧ بلغ عدد الطلبات ٨٠,٠٠٠ طلب، والفيسبوك توسعت في ذلك لتسمح لأي حكومة في العالم بالتقدم لطلبات مماثلة.

التطبيق العملي:

نبدأ من نوع المتصفح نفسه، نوع المتصفح الذي نحتاج هو ذلك النوع الذي يسمح لك بالتعديل عليه وإضافة وسائل امان له وبذلك نقصد المتصفحات مفتوحة المصدر مثل موزيلا فايرفوكس وجوجل كروم، ومتصفحات أخرى مبنية على هاذين المتصفحين، مثال على بعض المتصفحات التي ينصح بها:

اسم المتصفح	الرمز	درجة الأمان
tor browser		درجة الأمان عالية جدا وكذلك يشفر الاتصال بالنت – المتصفح مبني على الفايرفوكس
epic privacy browser		درجة الأمان عالية جدا ويعمي الأي بي الحقيق للمستخدم – المتصفح مبني على الكروم
IceDragon Inter-net Browser		درجة الأمان متوسط – المتصفح مبني على الكروم

يُتبع ›››

وينصح بشدة للمجاهدين ألا يستخدموا غير متصفح التور في نشاطاتهم عبر الشبكة العنكبوتية، لتوفره على درجة أمان عالية جدا.

لكن للمستخدم العادي فسيتم التطرق الى كيفية التعديل على متصفح الفايرفوكس لجعله أكثر امانا للاستخدام وذلك عن طريق تثبيت إضافات امنية عليه:

اسم الإضافة	الرمز	كيفية العمل / الدور
NoScript Security Suite		وهي إضافة مفيدة تمنع السكريتات التي قد تحمل ثغرات خطيرة أو هي بنفسها قد يكون عملها جمع المعلومات عن المستخدم وكذلك تمنع الجافا، ويمكن بسهولة ضد الإضافة للسماح لبعض المواقع الموثوقة من تشغيل السكريتات أو الجافا
Ghostery		يظهر للمستخدم من يتتبع نشاط المتصفح ويحظره
BetterPrivacy		يقضي على (الكوكيز) التابعة ل جوجل واليوتيوب ومواقع أخرى وتهدف الى جمع معلومات عن جهاز ونشاط المستخدم
Disconnect	D.	يعمل على منع إضافات تويتر والفيسبوك من جوجل من تتبع نشاط المستخدم ونتيجة لذلك أن يسرع عملية فتح المواقع والتصفح
HTTPS Everywhere		يجبر المواقع على الفتح عن طريق البروتوكول الآمن https ويؤمن اتصال مشفر بين الموقع والمستخدم

تذكر أخي المجاهد أنه لا يوجد برنامج أو متصفح يمكن ان يحميك ١٠٠٪ إن كنت أنت مستهتر بأمنك الشخصي، وتصر ان تكشف نفسك أو أعطيت المخترق معطيات اختراقك، ووضعت معلوماتك على العلن وحذاري من مواقع التواصل الاجتماعي ان تضع فيها معلوماتك الكاملة، أو التحدث بحرية على تطبيقات التراسل فيها، وان كنت متيقن من الطرف الآخر فكن كتيقن أيضا ان الموقع يخزن كافة نشاطاتك ومحادثاتك وقد يسلمها باي لحظة لأي جهة رسمية.

لمزيد من المعلومات يمكنكم التواصل مع الأخ: قسورة

@qswrh04myx



كيف تحمي جهازك الشخصـــي (٣)

بقلم: قسورة حفظه الله

الحمد لله والصلاة والسلام على رسول الله، أما بعد...

في الدروس السابقة من هذه السلسلة تطرقنا إلى كيفية حماية جهاز الحاسوب من الإختراق والتجسس واستكمالا لما سبق فسيكون هذا الدرس عن حماية البيانات والملفات الخاصة داخل الجهاز والذي يمكن الوصول إليها عن طريق الدخول المباشر للجهاز مثل عمليات التفتيش والمصادرة او حتى السرقة والاختراق، ولمن فاته الدروس السابقة يمكنه الرجوع الى العدد السابق من مجلة الوعد الآخر.

~~أولا: التجسس عليك عن طريق نظام التشغيل (الويندوز)~~

~~ثانياً: تأمين تصفح الإنترنت (تأمين المتصفح)~~

ثالثا: تشفير وتأمين البيانات (التعمية)

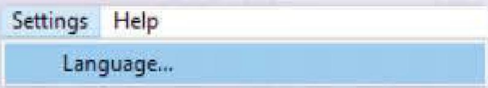
ما هو التشفير (التعمية): عبارة عن عملية تحويل البيانات والمعلومات من شكلها الحالي المجرد الى مجموعة من الرموز العشوائية بحيث تصبح غير مقروءة لأحد سوى من يملك صلاحية فك هذه الرموز السرية، وهو المستخدم الذي يملك مفتاح وخريطة هذه الرموز لتحويلها مرة أخرى الى شيء مقروء ومفهوم.

أهمية التشفير: تشفير البيانات والملفات هي الطريقة الوحيدة التي تمكن صاحبها من إخفاء المعلومة بنسبة ١٠٠٪، ولا يمكن إعادة فك التشفير إلا بإهمال من المستخدم نفسه، مثل كلمة سر ضعيفة أو استخدام برنامج تشفير مزور أو إختراق الجهاز للوصول لكلمة المرور أو حتى إعطاء كلمة مرور فك التشفير لشخص غير أمين.

برنامج التشفير

يوجد الكثير من برامج التشفير المنتشرة لكن من أفضلها هي البرامج التي تكون مفتوحة المصدر، وفي هذه الدرس سنشرح بإذن الله برنامج VeraCrypt، ويتم تنزيله من الرابط veracrypt.codeplex.com

بعد تنزيل البرنامج، ومن الواجهة الرئيسية نختار تغيير اللغة إلى العربية كي يسهل استخدامه وذلك عبر الذهاب الى <settings>language ونختار العربية كلغة لواجهة البرنامج



خطوات إنشاء حاوية (خزنة) ملفات مشفرة:



نصحك يا أخي المجاهد أن تقوم بإنشاء حاوية صغيرة للتجريب قبل عمل حاوية كبيرة.

١. نضغط على زر انشئ مجلد .



٢. تظهر لنا ٣ خيارات وهي:

أ- «أنشئ ملفاً حاويا معمى»: ونستخدم هذه الخيار لإنشاء مجلد مشفر يحوي بداخله الملفات التي تريد إخفائها، ويمكن تشبيه هذا المجلد بالخزنة الآمنة والتي يمكن فتحها لإدخال او اخراج الملفات ومن ثم إغلاقها.

ب- «عمّ غير مجلد/سواقة النظام»: وهذا الخيار لتشفير قرص كامل داخلي او خارجي أو بطاقة ذاكرة او فلاشه.

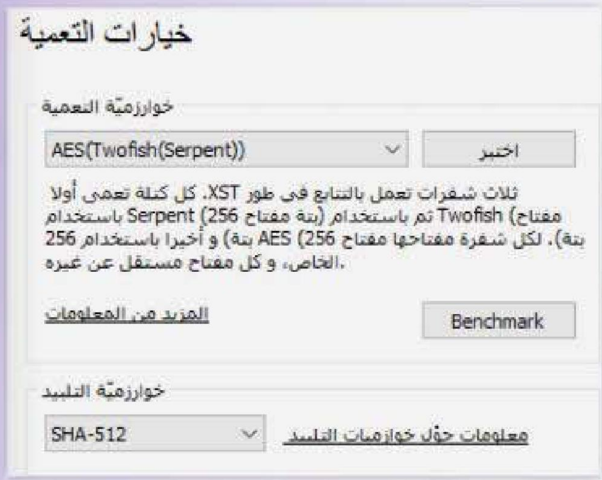
ج- «عمّ قسم النظام ...»: وهذا الخيار لتشفير القرص الذي عليه نظام التشغيل، ويسبب ذلك تشفير الويندوز نفسه، فلا يمكن الولوج إليه إلا عن طريق فك التشفير في كل مرة، نختار الخيار الأول ثم نضغط زر اللاحق.



٣. تظهر نافذة فيها خياران حول نوع المجلد أو الحاوية، اقرأ الخيارات الموجود في النافذة واختر ما يناسبك، علما بأنك إذا اخترت الخيار الثاني سوف تعيد العملية مرتين لإنشاء مجلد مخفي داخل المجلد المشفر. هنا اخترنا الخيار الأول.

يُتبع >>>

٤. بعد الضغط على زر اللاحق تنتقل الى نافذة تطلب منك تحديد المكان واسم المجلد المشفر، اختر مكان مخفي مثل أن يكون بين ملفات نظام التشغيل او داخل مجلد البرامج، وتجنب الأماكن الظاهرة مثل سطح المكتب والمستندات، وكذلك اختر اسم لا يلفت الانتباه مثل (خاص او سري أو ملف مشفر .. الخ) ولكن اختر اسم غير ملفت مثل windows7.iso أو backup او fted3g.dll ... الخ

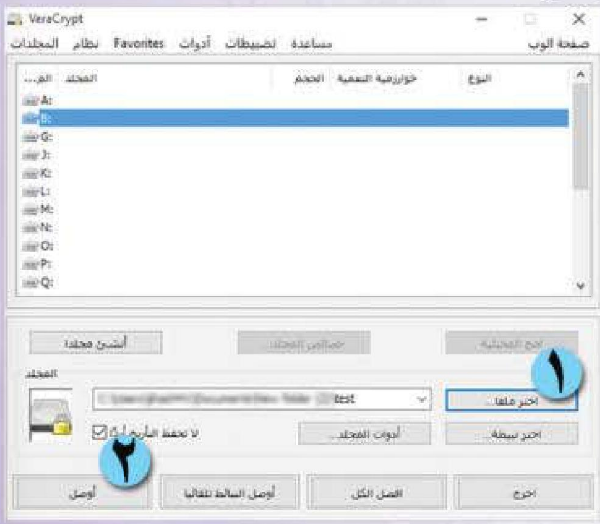


٥. النافذة التالية فيها خيارات التعمية كما في الصورة الجانبية نختار كما هو موضح وهي أقوى الخيارات الموجودة، ونختار اللاحق.

٦. يتم اختيار حجم المجلد المشفر.

٧. هنا يطلب كلمة مرور لفك تشفير المجلد وإعادة التشفير، يجب الاهتمام بشكل جدي بموضوع كلمة المرور لأنها الطريقة الوحيدة التي يمكن لحاملها الولوج للمجلد المشفر، فإذا سقطت بيد العدو او يد غير أمينة، أصبحت ملفاتك الخاصة مكشوفة.

٨. النافذة التالية يطلب من المستخدم تحريك المؤشر بشكل عشوائي داخل النافذة لأطول مدة وذلك لتوليد العمليات الحسابية العشوائية الخاصة بتشفير المجلد، حرك لمدة لا تقل عن دقيقة ثم اختر هيء، قد تطول عملية التهيء وذلك حسب حجم المجلد المشفر الذي اخترته. وبذلك تكون قد حصلت على مجلد مشفر يمكنك أن تستخدمه كحاوية أو خزنة لإخفاء ملفاتك.



خطوات فك وإعادة تشفير المجلد:

١. من النافذة الرئيسية يتم الضغط على زر اختيار ملف كما هو موضح في الصورة الجانبية، وإن كان المشفر عبارة عن قرص صلب فيتم الضغط على الزر الذي يقع أسفله مباشرة.

٢. عند الضغط على زر «أوصل» تفتح نافذة فيها إدخال كلمة مرور فك التشفير، تنتظر قليلا ومن ثم يفتح المجلد المشفر، وتراه موجود بجوار أحد الأحرف الموجودة في القائمة الموجودة في واجهة البرنامج، بالضغط المزدوج عليه يمكن إضافة او إزالة ملفات وحتى تحرير الملفات وحفظها.

٣. بعد الانتهاء من الضروري إغلاق الملف المشفر عن طريق نفس البرنامج وذلك عن طريق الضغط على زر «افصل».



تنبيهات مهمة:

- من المهم جدا قطع الاتصال بالأنترنت عند فتح أو إغلاق أي حاوية مشفرة، وذلك من باب الاحتياط في حال وجود إختراق خفي، وهذا يُقدر حسب أهمية المجلد بالنسبة لك.
- بعد غلق المجلد المشفر من المهم تنظيف الرام (الذاكرة المؤقتة) مباشرة وذلك عن طريق أحد برامج تنظيف الرام او إعادة تشغيل الجهاز، وذلك لأن الرام تحتفظ بكلمة السر التي كتبتها في لحين إعادة التشغيل او المسح.
- راجع الدرس الأول من هذه السلسلة عن كيفية تامين نظام التشغيل من برمجيات التجسس والفيروسات، وذلك ضروري حتى لا يكون عندك أي ثغرات أمنية تسمح للمختر ق الحصول على كلمة مرور المجلد.

لمزيد من المعلومات يمكنكم التواصل مع الأخ: قسورة

@qswrh04myx

كيف تحمي جهازك الشخصــي (٤)

بقلم: قسورة حفظه الله

الحمد لله والصلاة والسلام على رسول الله، أما بعد...

~~أولا: التجسس عليك عن طريق نظام التشغيل (الويندوز)~~
~~ثانياً: تأمين تصفح الإنترنت (تأمين المتصفح)~~
~~ثالثا: تشفير وتأمين البيانات (التعمية)~~

رابعا: مسح آثارك من الجهاز

يقصد بعملية مسح آثار المستخدم هو مسح أي بواقي لعلامات تدل على نشاط معين قمت به على جهازك الشخصي تدل عليك أو على معلومات تخصك، وهنا لا نقصد بعمليات الحذف التقليدي، بل بعمليات المسح المتقدمة.

ما هي الآثار التي يجب أن تحترس منها؟

- آثار الملفات المحذوفة: عند حذف أي ملف من النظام فإنه يبقى موجود في الخفاء الى أن يتم الكتابة فوقه والذي تم حذفه هو تعريف وجوده فقط والذي يدل على مكانه وحجمه وحجز مكانه على القرص الصلب، ويمكن بسهولة استرجاع ذلك الملف بإستخدام برامج خاصة.
- آثار الملفات المفتوحة: يحتفظ نظام التشغيل (الويندوز) بنسخة عن معظم الملفات التي تم فتحها مؤخرا!
- آثار الصور المصغرة (thumbnails): كل صورة تم فتحها أو حتى المرور عليها ينشئ نظام الويندوز نسخة مصغرة عن هذه الصورة ويحتفظ فيها بين الملفات المخفية وتبقى موجودة حتى لو حُذفت الصورة، وذلك ليسهل على المستخدم معاينة الملف قبل فتحه.
- آثار البيانات الوصفية (metadata): الكثير من الملفات وخاصة الصور، تحمل بيانات وصفية، فيها حجم الصورة وتاريخ التقاطها ونوع الكاميرا التي تم استخدامها أو نوع الجوال وسيريال الكاميرا/الجوال وفي بعض الأحيان يحتوي معلومات عن المكان الجغرافي وعند التصوير بالجوالات الحديثة يتم تسجيل إحداثيات المكان في حال كان خيار ال GPS مفعل، ومعلومات أخرى مثل صاحب الكاميرا/الجوال (إن كان اسمه مسجل على ذلك الجهاز) وكمية الإضاءة والكثير من البيانات التي تدل على صاحبها أو مكان الالتقاط أو حتى نوع الكاميرا.
- الملفات المؤقتة (temporary files): هذا المجلد يحتوي على نسخة من معظم الملفات التي يتم تحميلها من النت وخاصة عندما يتم تحميل ملف واختيار (فتح الملف مع عدم الحفظ)، لكن حقيقة الأمر أن الملف يتم حفظه في مجلد (temp) الى أن يتم حذفه.
- آثار التصفح وال cookies: كما أن النظام يخزن ويسجل جميع نشاطات المستخدم وكذلك الأمر بالنسبة للمتصفح حيث يحتفظ بنشاط تصفحك على الشبكة.
- آثار الحافظة: أن عمليات النسخ واللصق التي يقوم بها المستخدم يتم حفظها لحين استخدامها وعادة تظل محفوظة حتى إعادة تشغيل الجهاز، يمكن أن يكون ذلك المحفوظ كلمة سر أو نص أو صورة ...الخ
- الملفات المؤقتة للبرامج: كمان أن الويندوز يحفظ ملفات مؤقتة وكذلك البرامج مثل محرر النصوص أو الصور والسكايب ومشغل الوسائط على سبيل المثال لا الحصر، فإنها أيضا تحتفظ بنُسخ عن الملفات التي تم إستخدامها في تلك البرامج.

الوقاية:

ERASER

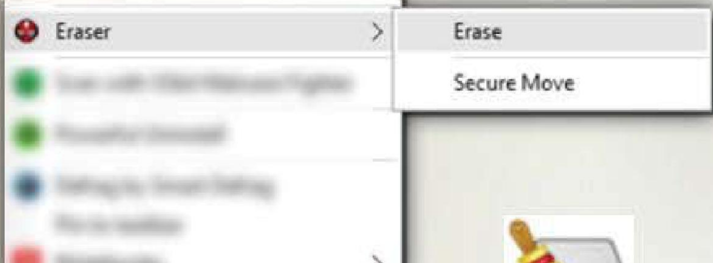
- الحذف الآمن للملفات:

من أبسط اشكال الحذف الآمن للملفات هو استخدام برامج تقوم بحذف الملف ثم الكتابة فوقه ببيانات عشوائية لا معنى لها، ومن البرامج السهلة المستخدمة Eraser، ويمكن تحميله من الرابط: eraser.heidi.ie

وهو معد افتراضيا أن يكتب فوق الملف ٣٥ مرة، وهو أيضا سهل الإستخدام، فبمجرد تنزيل البرنامج من موقعه، يندمج بشكل تلقائي في النظام، وعندما نريد حذف ملف أو مجلد فيتم الضغط عليه بزر الفأرة الأيمن لنجد اسم البرنامج ضمن القوائم ونختار الخيار الأول (Erase) كما في الصورة التالية:

يُتبع >>>

ثم تظهر نافذة تطلب تأكيد قبل عملية المسح، مجرد ما يتم تأكيد العملية تبدأ عملية المسح والكتابة في الخلفية، وقد تأخذ العملية وقتاً وذلك حسب حجم الملف وسرعة الجهاز.



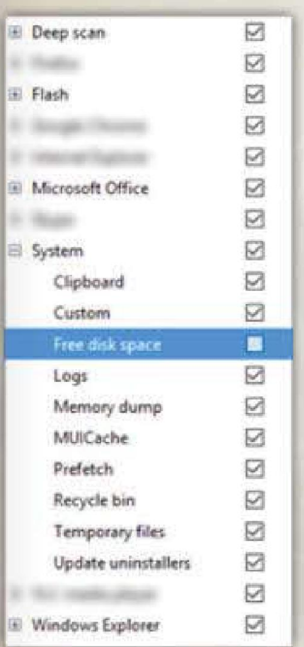
مع العلم أنه يمكن للمستخدم المتقدم من التحكم بعدد مرات الكتابة وتأجيل عملية المسح الى وقت معين وكذاك نوع البيانات المراد استبدالها مكان الملف، وذلك كله في اعدادات البرنامج.

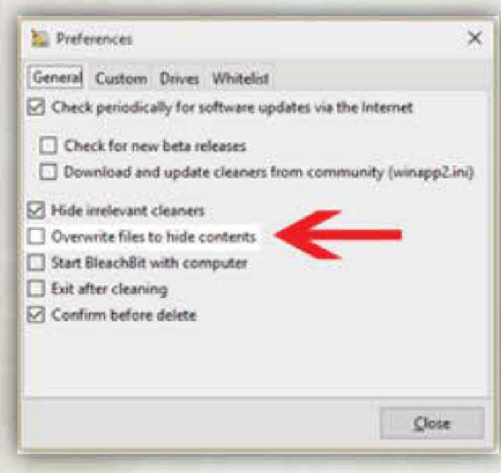


- **حذف الملفات المؤقتة (temporary files) والصورة المصغرة (thumbnails) وآثار التصفح وغيرها:**

سنستخدم لهذه العملية برنامج (BleachBit) ويمكن تحميله من الرابط: bleachbit.sourceforge.net

عند تنزيل البرنامج وفتحه، ستظهر القائمة التالية (كما في الصورة المقابلة)، وهي لتحديد ماذا يريد المستخدم تنظيفه من الجهاز، يمكن للمستخدم المتقدم أن يختار ما يريد مسحه بالتفصيل، لكن للمستخدم العادي فيمكن تحديد كافة الخيارات، مع استثناء الخيار Free disk space، لأن هذا الخيار يعمل على كتابة بيانات عشوائية على المساحات الفارغة في القرص الصلب وذلك لمسح أثر أي ملف تم حذفه من قبل، وهو نفس ما يقوم به البرنامج Eraser لكن هنا بشكل موسع ليشمل كل المساحة الفارغة على القرص، فهذه العملية قد تستهلك وقت طويل (من نصف ساعة الى عدة ساعات حسب الحجم الفارغ المراد تنظيفه)، ومع ذلك بفضل استخدامه مرة واحدة.

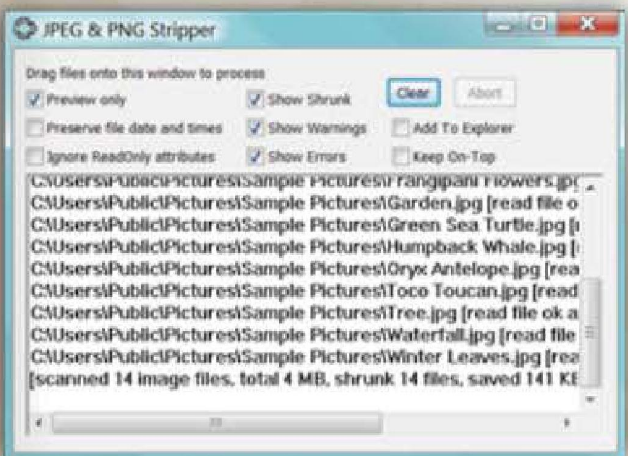




عند تحديد كافة الخيارات، ستظهر بعض النوافذ التحذيرية لبعض عمليات المسح أنها ستأخذ وقت، وبعض النوافذ تحذر المستخدم من ان أي كلمة سر مُخزنة في المتصفح سيتم حذفها، نضغط موافق.

بعد تحديد الخيارات وقبل البدء بالتنظيف، ندخل الى اعدادات البرنامج من قائمة edit>preferences ويتم تحديد الصندوق المجاور ل Overwrite files «to hide contents» كما في الصورة، ويعني ألا يكتفي البرنامج بحذف الملفات بل الكتابة فوقها حتى لا يتم استرجاعها، وهذا أمر مهم، ثم نختار البدء بعملية التنظيف عن طريق الضغط على زر clean أعلى يسار نافذة البرنامج.





- **البيانات الوصفية من الصور:**

نستخدم لهذه العملية برنامج صغير وبسيط يسمى JPEG & PNG Stripper ويمكن تحميله من الرابط: steelbytes.com/?mid=٣٠، وهو يتعامل مع ملفات ذات امتداد jpeg وpng ولا يحتاج تثبيت وكل ما على المستخدم فعله هو فتح البرنامج وتحديد الصور ثم اسقاطها في نافذة البرنامج وهو يعمل تلقائيا على تنظيف الصور.